IN THE CLAIMS:

Claims 1-24 (Canceled).

25. (Currently Amended) A secure network having a plurality of host computers accessible to users and connected to a network medium that has access to an untrusted line, the secure network comprising:

a network security controller for enabling a security officer to generate at least one user profile for each user and for sending at least one user profile to security devices connected to the network medium, each user profile defining at least one destination which the user is authorized to access through discretionary access control and mandatory access control security mechanisms, wherein a plurality of user profiles define virtual private networks of communication comprising subsets of host computers; and,

security devices connected to the network medium for receiving the user profiles generated at the network security controller and for implementing security mechanisms associated with the user profiles, each security device associated with one host computer, each security device having an authorization device for authorizing users at the associated host computer, the security device permitting the authorized user, via the associated host computer, to select a user's profile associated with the user and for restricting access of the host computer to the at least one destination defined in the selected user's profile.

26. (Original) The network of claim 25, wherein the at least one destination comprises at least one other host computer of the network or the untrusted line.

27. (Currently Amended) The network of claim 25, wherein the security device, when implementing security mechanisms, allows~~when~~ the host computer ~~connects~~ to connect to a trusted destination.

28. (Original) The network of claim 25, the security device not implementing security mechanisms when the host computer connects to an untrusted destination.

29. (Original) The network of claim 25, wherein the untrusted line comprises the Internet.

30. (Original) The network of claim 25, wherein a user cannot simultaneously communicate with a trusted destination and an untrusted destination.

31. (Original) The network of claim 25, wherein a user is prevented from simultaneously connecting to destinations having different security levels.

32. (Original) The network of claim 25, wherein a user can only select one profile at a time.

Claim 33 (Canceled).

34. (Original) The network of claim 25, wherein security is implemented at a network layer of protocol hierarchy.

35. (Original) The network of claim 25, wherein at least one user profile has only one destination.

36. (Original) The network of claim 25, wherein the destination in a user's profile correspond to a level of security granted the user.

37. (Original) The network of claim 25, wherein the security devices are integrated with the associated host computer.

38. (Amended) A method for operating a network having a plurality of host computers accessible to users and connected to a network medium that has access to an untrusted line, the method comprising:

generating at least one user profile for each user, each user profile defining at least one destination which the user is authorized to access through discretionary access control and mandatory access control security mechanisms, to define virtual private networks of communication comprising subsets of host computers;

authorizing a user at a host computer;

determining, at the host computer, the at least one user profile associated with the authorized user;

permitting, at the host computer, the authorized user to select a user's profile associated with the user; and

restricting access of the host computer to the at least one destination defined in the selected user's profile.

39. (Original) The method of claim 38, wherein the at least one destination comprises at least one other host computer of the network or the untrusted line.

40. (Currently Amended) The method of claim 38, further comprising the step of implementing a security mechanism ~~when~~to enable the host computer ~~connects~~to connect to a trusted destination.

41. (Original) The method of claim 38, further comprising the step of not implementing security mechanisms when the host computer connects to an untrusted destination.

42. (Original) The method of claim 38, wherein the untrusted line comprises the Internet.

43. (Original) The method of claim 38, wherein a user cannot simultaneously communicate with a trusted destination and an untrusted destination.

44. (Original) The method of claim 38, wherein a user is prevented from simultaneously connecting to destinations having different security levels.

45. (Original) The method of claim 38, wherein a user can only select one profile at a time.

Claim 46 (Canceled).

47. (Original) The method of claim 38, wherein security is implemented at a network layer of protocol hierarchy.

48. (Original) The method of claim 38, wherein at least one user profile has only one destination.

49. (Original) The method of claim 38, wherein the destination in a user's profile correspond to a level of security granted the user.

50. (Original) A multi-level secure network having a plurality of host computers accessible to users and connected to a network medium that has access to an untrusted line, the secure network comprising a security device coupled between at least one host computer and the network medium which operates at a network layer communications protocol and a network security controller for controlling the security device to establish connections to the network medium.

51. (Original) The multi-level secure network of claim 50, wherein the network security controller audits events.

52. (Original) The multi-level secure network of claim 50, wherein the security device prevents simultaneous connection to a trusted line and an untrusted line.

53. (Original) The multi-level secure network of claim 50, wherein the security device prevents simultaneous connection between lines of different security levels.

54. (Previously Presented) A secure network having a plurality of host computers accessible to users and interconnected with a non-secure communication medium such as the Internet, the secure network comprising:

a network security controller for enabling a security officer to generate at least one user profile for each user, each user profile defining at least one destination which the user is authorized to access; and,

security devices connected with said host computers for receiving the user profiles generated at the network security controller, each security device associated with one host computer, each security device having an authorization device for authorizing users at the associated host computer, the security device permitting the authorized user, via the associated host computer, to select a user's profile associated with the user and for restricting access of the host computer to the at least one destination defined in the selected user's profile, and wherein each security device includes a communication control system to control access of the host computer to the communication medium, said communication control system including a data storage device for storing data provided by said host computer in a memory space, and for transferring data out of said memory space while making the transferred data inaccessible to said host computer.

55. (Previously Presented) A security device for a multi-level secure network implementing security at a network layer (layer 3) of protocol hierarchy having a plurality of host computers accessible to users for communication over a computer network medium, said security device locatable between said host computer and the network medium, wherein said security device comprises a network interface for connecting said security device to the network medium, and a port for connecting said security device to said host computer and further comprising a memory device connected with said port for storing data provided from said host computer in a memory space, and means for switching said data out of said memory space while making said switched data inaccessible to said host computer, thus controlling the pass-through of data between said host computer and the network medium.

56. (Previously Presented) A security device for a multi-level secure network implementing security at a network layer (layer 3) of protocol hierarchy having a plurality of host computers accessible to users and connected to a computer network medium, said security device connectable between at least one host computer bus and the network medium, said security device comprising

a local bus, a local RAM, and a local processor;

a network interface for connecting said local bus to the computer network medium and including a network processing means for transferring information between said local RAM and said network medium;

a communication separation means for connection between said local bus and said host bus and for preventing direct pass-through of information between said host bus and said local

bus and for preventing direct access between said host bus and said local RAM, said communication separation means including a memory device for storing information provided over said host bus in a memory space, a first port interconnecting said host bus and said memory device, and a second port interconnecting said local bus and said memory device, said information transferrable from said memory space to said local bus while making the transferred information inaccessible to said host bus;

wherein said local processor processes information to be transferred between said host bus and said network medium in accordance with a predetermined security policy to determine whether communication between a host computer and the network medium is authorized, said local processor including means for accessing host bus information from said memory space and transferring said information to said local bus.

57. (Previously Presented) The security device of claim 56 wherein said local processor processes said host bus information in accordance with said predetermined security policy, transfers the processed host bus information to said local RAM for access by said network processing means, accesses network medium information placed in said local RAM by said network processing means, processes said network medium information in accordance with said security policy, and transfers the processed network medium information to said communication separation means for access by said host bus.

58. (Previously Presented) A security device for connecting a host computer from a host bus to a computer-accessible network, the security device comprising a local bus, a network interface

for connecting said local bus to the computer-accessible network, and a communication separation and control system for connection between said local bus and said host bus, said communication separation and control system including a first port coupled to said host bus, a second port coupled to said local bus, and a signal storage device interconnecting said first and second ports, said signal storage device storing signals provided over said host bus in a host bus memory space and over said local bus in a local bus memory space, wherein said signals are transferable between said host bus memory space and said local bus memory space with said switched signals from said host bus memory space being invisible to said host bus after being switched to said local bus memory space, said communication separation and control system preventing pass-through of signals between said host bus and said computer-accessible network without transitory storage in said signal storage device, and further comprising security device processing means for controlling the transfer of signals out of said local bus memory space of said signal storage device.

59. (New) The secure network of claim 25 wherein said network security controller includes means for changing user profiles and sending updated user profiles to said security devices.

60. (New) A method for controlling a sending computer to transmit information to a receiving computer over a computer network, the method comprising:

providing a security device at each sending computer and receiving computer;

receiving the information from the sending computer at the sending computer security device to be transmitted to the receiving computer;

implementing security mechanisms at a network layer of ISO protocol hierarchy to determine whether communication is authorized from the sending computer to the receiving computer by determining if the receiving computer is in a transmit list and consistent with a transmit security window through discretionary access control and mandatory access control, respectively and, if either condition is not satisfied then terminating the transmission of information, otherwise encrypting the information to be transmitted; and

transmitting the encrypted information to the security device of the receiving computer over the computer network.

61. (New) The method of claim 60 further comprising the step of setting user identification information at each security device for enabling a user to access the computer associated with the security device.

62. (New) The method of claim 61 further comprising the step of providing a network security controller on said computer network for receiving from said security device the identification of an authorized user and establishing one or more user profiles at each security device for said authorized user.

63. (New) The method of claim 62 further comprising providing security mechanisms from said network security controller to said security devices including providing discretionary access control and mandatory access control policies for each user profile.

64. (New) The method of claim 63 further comprising the step of auditing the termination of transmission of information at the network security controller.

65. (New) The method of claim 60 wherein said security device is a software implementation incorporated within one or more of the sending and receiving computers.

66. (New) The method of claim 63 wherein said computer network includes an untrusted network such as the Internet.

67. (New) The method of claim 66 wherein each security device prevents simultaneous connection at different security levels established by mandatory access controls.

68. (New) The method of claim 66 wherein each security device prevents simultaneous connection to trusted and untrusted networks.

69. (New) A method for controlling a sending computer to transmit information to a receiving computer over a computer network, the method comprising:

providing a security device at each sending computer and receiving computer;

setting user identification information at each security device for enabling a user to access the computer associated with the security device;

providing a network security controller on said computer network for receiving from said security device the identification of an authorized user and for establishing one or more

user profiles at each security device for said authorized user, including providing discretionary access control and mandatory access control policies for each user profile;

receiving information to be transmitted from the sending computer to the receiving computer at the sending computer security device;

implementing security mechanisms at a network layer of ISO protocol hierarchy to determine whether communication is authorized from the sending computer to the receiving computer by determining if the receiving computer is in a transmit list and consistent with a transmit security window through discretionary access control and mandatory access control, respectively and, if either condition is not satisfied then terminating the transmission of information and sending termination notice to the network security controller, otherwise encrypting the information to be transmitted; and

transmitting the encrypted information to the security device of the receiving computer over the computer network.

70. (New) The method of claim 69 further comprising the step of changing user profiles at the network security controller and updating available user profiles at a security device.

71 (New) The method of claim 69 further comprising the step of auditing the termination of transmission of information at the network security controller.

72. (New) The method of claim 69 wherein said security device is a software implementation incorporated within one or more of the sending and receiving computers.

73. (New) The method of claim 69 wherein said computer network includes an untrusted network such as the Internet.

74. (New) The method of claim 69 wherein each security device prevents simultaneous connection at different security levels established by mandatory access controls.

75. (New) The method of claim 69 wherein each security device prevents simultaneous connection to trusted and untrusted networks.

76. (New) A method for controlling a receiving computer to receive information transmitted from a transmitting computer over a computer network, the method comprising:

providing a security device at each transmitting computer and receiving computer;

receiving information from the computer network at the receiving computer security device;

implementing security mechanisms at a network layer of ISO protocol hierarchy to determine whether communication is authorized from the transmitting computer to the receiving computer by determining if the receiving computer is in a receive list and consistent with a receive security window through performing discretionary access control and mandatory

access control, respectively and, if either condition is not satisfied then terminating the reception of information, otherwise decrypting the information to be received; and

transmitting the decrypted information from the receiving computer security device to the receiving computer for reception thereof.

77. (New) The method of claim 76 further comprising the step of providing a network security controller on said computer network for providing security mechanisms to said security devices including discretionary access control and mandatory access control policies.

78. (New) The method of claim 77 further comprising the step of auditing the termination of reception of information at the network security controller.

79. (New) A method for controlling a receiving computer to receive information transmitted from a transmitting computer over a computer network, the method comprising:

providing a security device at each transmitting computer and receiving computer;

setting user identification information at each security device for enabling a user to access the computer associated with the security device;

providing a network security controller on said computer network for receiving from said security device the identification of an authorized user and establishing one or more user profiles at each security device for said authorized user and providing security mechanisms to said security devices including discretionary access control and mandatory access control policies for each user profile;

receiving information transmitted by the transmitting computer, via a security device, on the computer network at the receiving computer security device;

implementing security mechanisms at a network layer of ISO protocol hierarchy to determine whether communication is authorized from the transmitting computer to the receiving computer by determining if the receiving computer is in a receive list and consistent with a receive security window through performing discretionary access control and mandatory access control, respectively and, if either condition is not satisfied then terminating the reception of information, otherwise decrypting the information to be received;

transmitting the decrypted information from the receiving computer security device to the receiving computer for reception thereof; and

auditing the termination of reception of information at the network security controller.

80 (New) The method of claim 79 further comprising the step of changing user profiles at the network security controller and updating available user profiles at a security device.

81. (New) The method of claim 79 wherein said security device is a software implementation incorporated within one or more of the sending and receiving computers.

82. (New) The method of claim 79 wherein said computer network includes an untrusted network such as the Internet.

83. (New) The method of claim 79 wherein each security device prevents simultaneous connection at different security levels established by mandatory access controls.

84. (New) The method of claim 79 wherein each security device prevents simultaneous connection to trusted and untrusted networks.